Building Secure Delivery Skills with DevSecOps Professional Certification

Introduction

Modern engineering teams must deliver software quickly while protecting applications, infrastructure, and user data.

The DevSecOps Certified Professional (DSOCP) certification helps learners understand how security can be included throughout development, testing, deployment, cloud operations, and production support.

It is suitable for developers, DevOps engineers, SREs, cloud professionals, security specialists, platform engineers, and technical managers.

Understanding DSOCP

DSOCP is a professional certification that brings development, operations, and security practices together.

It teaches learners how to identify risks earlier, automate security checks, protect credentials, review software dependencies, secure containers, validate infrastructure, and monitor production systems.

The main aim is to make security a regular part of software delivery rather than a final review.

Who Can Benefit from DSOCP?

The certification can support:

- Software developers
- DevOps engineers
- Cloud engineers
- Site reliability engineers
- Security professionals
- Platform engineers
- Technical leads
- Engineering managers
- Beginners with basic Linux, Git, and CI/CD knowledge

Main Skills Covered

DSOCP can help learners build knowledge in:

- Secure software development
- Static and dynamic application testing
- Dependency vulnerability analysis
- Secret and credential protection
- Container and Kubernetes security
- Infrastructure-as-code scanning
- Policy as code
- Vulnerability management
- Runtime monitoring
- Incident response
- Software supply-chain security

Certification Structure

The DSOCP program is provided by DevOpsSchool.

The learning process generally includes instructor guidance, demonstrations, practical labs, assignments, and certification assessment.

Track	Level	Who It Is For	Prerequisites	Skills Covered	Recommended Order
DevSecOps Foundation	Foundation	Beginners and junior professionals	Basic software and IT knowledge	Secure SDLC and security fundamentals	First
DevSecOps Certified Professional	Professional	Developers, DevOps, SRE, cloud, platform, and security professionals	Linux, Git, containers, and CI/CD basics	Security automation, scanning, policies, and monitoring	Second
Advanced	Advanced	Senior	Practical	Architecture	Third

Track	Level	Who It Is For	Prerequisites	Skills Covered	Recommended Order
DevSecOps		engineers, architects, and technical leads	DevSecOps experience	, governance, compliance, and supply-chain security	

Projects Learners Should Be Able to Complete

After completing DSOCP, learners should be able to:

- Add security checks to a CI/CD pipeline.
- Scan source code for weaknesses.
- Detect vulnerable third-party packages.
- Find exposed passwords, keys, and tokens.
- Check container images before deployment.
- Review infrastructure templates for unsafe settings.
- Apply automated deployment policies.
- Create a vulnerability-remediation process.
- Monitor security activity in production.

Preparation Roadmap

7-Day Plan

Review Linux, Git, networking, containers, CI/CD, and basic security concepts.

30-Day Plan

Practise code scanning, dependency analysis, secret detection, container security, and infrastructure validation.

60-Day Plan

Build one complete secure delivery project and practise handling realistic security findings.

Common Mistakes to Avoid

- Learning tools without understanding the risks
- Ignoring false positives

- Storing credentials in repositories
- Blocking every issue without reviewing severity
- Focusing only on code scanning
- Ignoring cloud and runtime security
- Failing to assign remediation ownership

Choose Your Learning Path

DevOps Path

Learn Linux, Git, CI/CD, containers, cloud platforms, and infrastructure automation before adding security practices.

DevSecOps Path

Study secure development, threat modelling, vulnerability management, and automated security controls.

SRE Path

Combine reliability, observability, incident response, and production operations with DevSecOps knowledge.

AIOps Path

Develop skills in anomaly detection, event analysis, automation, and secure operational governance.

MLOps Path

Protect model pipelines, APIs, containers, dependencies, secrets, and machine-learning infrastructure.

DataOps Path

Secure data pipelines, repositories, credentials, infrastructure, and access policies.

FinOps Path

Combine cloud cost control with identity, ownership, configuration, and security policies.

Why DSOCP Can Be Useful

DSOCP can help professionals understand how security fits into practical software-delivery workflows.

Its real value comes from learning how to identify risks, automate checks, review findings, and support remediation.

The certification should be combined with hands-on labs, personal projects, documentation, and troubleshooting practice.

Frequently Asked Questions

1. Is DSOCP suitable for beginners?

Yes. Basic Linux, Git, container, cloud, and CI/CD knowledge is recommended.

2. Is DSOCP only for security engineers?

No. It is also useful for developers, DevOps engineers, SREs, cloud teams, platform engineers, and managers.

3. Does DevSecOps slow software delivery?

Poorly designed controls can create delays. Automated and risk-based checks can improve security without unnecessary manual work.

4. Is DSOCP practical?

The learning approach generally includes demonstrations, labs, assignments, and realistic technical scenarios.

5. What can learners study after DSOCP?

They may continue with cloud security, Kubernetes security, application security, advanced DevSecOps, SRE, or security leadership.

Final Thoughts

DSOCP is a useful certification for professionals who want to strengthen secure software-delivery skills.

It can help learners understand application security, pipeline protection, container security, infrastructure scanning, policy enforcement, vulnerability management, and production monitoring.

For better results, learners should complete at least one end-to-end DevSecOps project alongside their certification preparation.